(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－44553

(43)公開日　平成８年(1996)２月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　9/06	５５０　Ｃ	7230－5B		
12/14	３２０　Ｂ			

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）

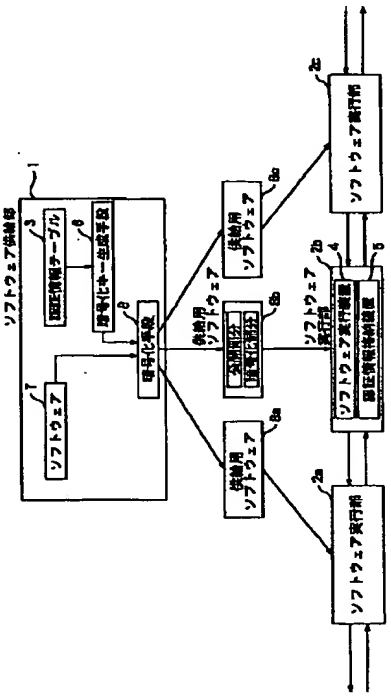
(21)出願番号　特願平6－182574

(22)出願日　平成６年(1994)８月３日

(71)出願人　000155469
株式会社野村総合研究所
東京都中央区日本橋１丁目10番１号
(72)発明者　真　下　竜　実
神奈川県横浜市保土ケ谷区神戸町134番地
株式会社野村総合研究所内
(72)発明者　小　野　喜代志
神奈川県横浜市保土ケ谷区神戸町134番地
株式会社野村総合研究所内
(74)代理人　弁理士　佐藤　一雄　（外３名）

(54)【発明の名称】　公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム

(57)【要約】
【目的】　公開部分についてはユーザーによる作成・流用を許し、非公開部分については正規に購入したユーザのみが使用できるソフトウェアを複数ユーザに使用させるシステムを提供する。
【構成】　認証情報に基づく暗号化キーによってソフトウェアの非公開部分を暗号化するソフトウェア供給部１と、演算処理装置９と、メモリ１０と、メモリ１０に対するアクセスを制御するメモリ制御装置１１と、各ユーザに固有の認証情報を格納する認証情報格納装置５と、表示装置１３と、入力手段１２とを有する複数のソフトウェア実行部２とからなり、ソフトウェア実行部２のメモリ制御装置１１に、ソフトウェアの非公開部分と公開部分を検出する暗号化検出回路１４と、認証情報格納装置５から認証情報を入力して復号化キーを生成して暗号化検出回路１４が検出したソフトウェアの非公開部分を復号化するデータ復号化回路１５とを備えた。



1

【特許請求の範囲】
【請求項１】正規のユーザに固有の認証情報に基づいて作成された暗号化キーによってソフトウェアの非公開部分を暗号化するソフトウェア供給部と、
演算処理装置と、前記演算処理用のメモリと、前記メモリに対するアクセスを制御するメモリ制御装置と、各ユーザに固有の認証情報を格納する認証情報格納装置と、表示装置と、入力手段とを有する複数のソフトウェア実行部とからなり、
前記ソフトウェア実行部のメモリ制御装置は、ソフトウェアの暗号化された非公開部分と公開部分を検出する暗号化検出回路と、前記認証情報格納装置から認証情報を入力して復号化キーを生成して前記暗号化検出回路によって検出されたソフトウェアの非公開部分を復号化するデータ復号化回路とを備えていることを特徴とする公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム。
【請求項２】前記ソフトウェアを前記メモリにロードする際に、前記暗号化検出回路によって検出された公開部分のプログラムあるいはデータを、前記メモリ上の参照可能領域にロードし、前記データ復号化回路によって復号化された非公開部分のプログラムあるいはデータを前記メモリ上の参照不可領域にロードするように前記メモリ制御装置を構成し、
前記メモリ制御装置に、参照不可領域のプログラムの実行による参照不可領域へのアクセス命令を許可し、参照可能領域のプログラムあるいは外部のプログラムの実行による参照不可領域へのアクセス命令を禁止するアクセス制御手段を備えたことを特徴とする請求項１に記載の公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム。
【請求項３】前記ソフトウェア供給部と前記複数のソフトウェア実行部は通信回線によって互いに連結されていることを特徴とする請求項１または請求項２に記載の公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は公開部分と非公開部分とを有するソフトウェアを多数のユーザに使用させるシステムに係り、特にソフトウェアの基本的な動作を規定する雛型ソフト（非公開部分）とユーザの創意工夫によって作成・改変されるカスタマイズソフト（公開部分）とからなるソフトウェアにおいて、上記カスタマイズソフトについてはユーザ間で自由に流用できるようにし、雛型ソフトについてはその雛型ソフトを正規に購入したユーザのみが使用できるようにしたシステムに関する。
【０００２】
【従来の技術】従来から内容を秘密にしようとするソフトウェアを多数のユーザに使用させる場合には、ソフトウェアの一部に各ユーザ固有の認証情報を付加し、これをプログラム実行中に正規ユーザによる使用か否かを繰り返しチェックする方法と、ソフトウェア供給者側でソフトウェアを暗号化して出荷し、ユーザ側で復号化キーを入力してソフトウェアを復号化して使用する方法等があった。以下これらの従来の技術について詳しく説明する。
【０００３】図４は、プログラムの一部に各ユーザの固有の認識情報を付加し、これをプログラム実行中に正規ユーザによる使用か否かを繰り返しチェックするシステムを示している。
【０００４】この従来のシステムは、ソフトウェア供給者が所有するソフトウェア供給部２１と、契約等によってソフトウェアの供給を受けて使用するユーザが所有する複数のソフトウェア実行部２２とからなる。ソフトウェア供給部２１は供給用のプログラム２３と、登録したユーザのソフトウェア実行部に固有の認証情報２４を有し、ユーザの要求により、認証情報付加手段２５によってそのユーザが希望する供給プログラム２３の一部にそのユーザに固有の認証情報２４を付加して、供給用のプログラム２６としてユーザに供給する。
【０００５】一方、ソフトウェア実行部２２は、ソフトウェアを実行するソフトウェア実行手段２７と、そのソフトウェア実行部に固有の認証情報を格納した認証情報記憶装置２８と、プログラムに付加された認証情報とそのプログラムを実行しているソフトウェア実行部の認証情報を比較判定する認証情報チェック手段２９とを有している。
【０００６】ユーザが認証情報を付加したプログラムをプログラム実行手段２７によって実行するとき、プログラムの所定位置には認証情報をチェックする命令と認証情報が格納されており、この部分を実行すると認証情報記憶装置２８から実行中のソフトウェア実行部２２の認証情報が読み出され、認証情報チェック手段２９によってプログラムとソフトウェア実行部２２の認証情報が比較される。
【０００７】認証情報が一致していれば、正規のユーザによる使用と判断され、一致していなければ不正な使用と判断されてプログラムの実行が停止される。これによって正規のユーザによる正規の使用を確保している。
【０００８】次に、プログラムを暗号化して供給し、ユーザ側で復号化して使用するシステムについて説明する。
【０００９】図５に示すように、本システムは図４のシステム同様に通常一つのソフトウェア供給部３１と複数のソフトウェア実行部２３とからなる。ソフトウェア供給部３１は、供給プログラム３３と各ソフトウェア実行部３２に固有の暗号化キー３４を格納しており、また、供給プログラム暗号化手段３５を備えている。ユーザの要求があったときに、ソフトウェア供給部３１は、その

2

ユーザの暗号化キー３４によって希望のあった供給プログラム３３を暗号化し、暗号化供給プログラム３６としてユーザに供給する。

【００１０】ソフトウェア実行部３２は、プログラム実行手段３７と、ユーザが復号化キーを入力するための復号化キー入力手段３８と、復号化キーによって暗号化されたプログラムを復号化する暗号化プログラム解読手段３９とを有している。

【００１１】供給された暗号化供給プログラム３６は、プログラム実行手段３７によって実行されると、最初にユーザに復号化キーの入力を求める。ユーザが復号化キー入力手段３８によって復号化キーを入力すると、暗号化プログラム解読手段３９が入力された復号化キーを用いて暗号化供給プログラム３６を復号して解読プログラム４０を生成し、プログラム実行手段３７が生成された解読プログラム４０を実行する。

【００１２】ユーザが正規に登録された者である場合、復号化キーは予めユーザに知らされており、この復号化キーによってプログラムは正常に復号化される。これに対してユーザが正規に登録していない場合、入力された復号化キーは暗号化キーと対応しないため、解読プログラム４０は実行不能のものとなる。

【００１３】

【発明が解決しようとする課題】上記供給プログラム中に各ソフトウェア実行部に固有の認証情報を付加する従来のシステムでは、プログラム毎に所定位置に認証情報を付加しなければならないので、供給者側で作業が煩雑であった。

【００１４】また、プログラム毎に認証情報を付加するため、プログラム毎に認証情報をチェックしなければならず、特に複数のプログラムを同時に利用するソフトウェアでは、認証情報チェック手段用の接続インターフェースもプログラムの数に対応して複数必要であるため、ソフトウェア実行部の構成が複雑であった。

【００１５】さらに、プログラム中の認証情報チェック部分をプログラム解析によってさがし当て、これを書き換えることによってチェック機能を無効にし、チェック機能を無効にしたプログラムを大量かつ不正に複製することができた。また、その他の問題として、上記方法はプログラムの実行中に周期的に認証情報をチェックするため、データには適用することができなかった。

【００１６】一方、上記ユーザに復号化キーを入力させてプログラムを復号化して実行させる従来のシステムでは、ユーザの意志によっては、プログラムを復号化した状態で複製される可能性があった。

【００１７】また、ユーザの意志によらない場合でも、復号化キーを試行錯誤的に入力して復号化キーを探り当てる可能性があり、一旦復号化キーを探り当てられると複製プログラムが大量に出回る可能性があった。

【００１８】また、上記ソフトウェアを多数のユーザに

使用させる従来のシステムのいずれによっても、一部に非公開部分を有し、一部に公開部分を有し、公開部分についてはユーザによる改変・新規作成、ユーザ間の流用を許し、非公開部分については正規に購入したユーザがのみが使用できるようするソフトウェアには適用できない。

【００１９】そこで、本発明の目的は、上記従来の課題を解決し、不正使用を防止し、公開部分についてはユーザーによる改変・新規作成およびユーザ間の流用を許し、非公開部分については正規に購入したユーザのみが使用できるようにしたソフトウェアを複数ユーザに使用させるシステムを提供することにある。

【００２０】

【課題を解決するための手段】上記目的達成のために、本願の請求項１に係る「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」は、正規のユーザに固有の認証情報に基づいて作成された暗号化キーによってソフトウェアの非公開部分を暗号化するソフトウェア供給部と、演算処理装置と、前記演算処理用のメモリと、前記メモリに対するアクセスを制御するメモリ制御装置と、各ユーザに固有の認証情報を格納する認証情報格納装置と、表示装置と、入力手段とを有する複数のソフトウェア実行部とからなり、前記ソフトウェア実行部のメモリ制御装置は、ソフトウェアの暗号化された非公開部分と公開部分を検出する暗号化検出回路と、前記認証情報格納装置から認証情報を入力して復号化キーを生成して前記暗号化検出回路によって検出されたソフトウェアの非公開部分を復号化するデータ復号化回路とを備えていることを特徴とするものである。

【００２１】本願の請求項２に係る「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」は、前記ソフトウェアを前記メモリにロードする際に、前記暗号化検出回路によって検出された公開部分のプログラムあるいはデータを、前記メモリ上の参照可能領域にロードし、前記データ復号化回路によって復号化された非公開部分のプログラムあるいはデータを前記メモリ上の参照不可領域にロードするように前記メモリ制御装置を構成し、このメモリ制御装置に、参照不可領域のプログラムの実行による参照不可領域へのアクセス命令を許可し、参照可能領域のプログラムあるいは外部のプログラムの実行による参照不可領域へのアクセス命令を禁止するアクセス制御手段を備えたことを前記ソフトウェアを前記メモリにロードする際に、前記暗号化検出回路によって検出された公開部分のプログラムあるいはデータを、前記メモリ上の参照可能領域にロードし、前記データ復号化回路によって復号化された非公開部分のプログラムあるいはデータを前記メモリ上の参照不可領域にロードするように前記メモリ制御装置を構成し、前記メモリ制御装置に、参照不可領域のプログラムの実行による参照不可領域へのアクセス命令を許可し、

5

参照可能領域のプログラムあるいは外部のプログラムの実行による参照不可領域へのアクセス命令を禁止するアクセス制御手段を備えたことを特徴とするものである。

【００２２】本願の請求項３に係る「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」は、上記第一あるいは第二の発明によるシステムにおいて、前記ソフトウェア供給部と前記複数のソフトウェア実行部は通信回線によって互いに連結されていることを特徴とするものである。

【００２３】

【作用】本願の請求項１による「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」によれば、各ユーザに固有の認証情報に基づいて作成された暗号化キーによってソフトウェアの非公開部分のみを暗号化する。これに対して、ソフトウェア実行部では、暗号化検出回路によって配布されたソフトウェアに対して暗号化された非公開部分を検出し、データ復号化回路によって各ユーザの認証情報に基づいて生成された復号化キーによって復号化する。

【００２４】この場合、前記データ復号化回路による復号化はソフトウェアの非公開部分については強制的に行なわれるように構成されている。すなわち、非公開部分についてどのような暗号化キーによって暗号化されているか、あるいはすでに解読されたプログラム・データであるかに拘らず、一律にそのソフトウェア実行部の認証情報に基づいて作成された復号化キーによって復号化する。

【００２５】これにより、一致しない認証情報の復号化キーによって復号化した場合は意味をなさないプログラム・データになるばかりでなく、すでに解読・復号化されたプログラム・データも復号化キーによって新に意味をなさないプログラム・データに変換される。

【００２６】すなわち、特定のソフトウェア実行部でソフトウェアを実行させるためには、そのソフトウェア実行部の認証情報に基づく暗号化キーによって暗号化したプログラム・データをそのソフトウェア実行部の所有者に渡さなければならないことになる。このことは、プログラム・データを一度解読すると大量に使用可能なプログラム・データを複製できる従来の技術の欠点を克服でき、不正な使用を効果的に防止することができる。

【００２７】また、上記復号化はソフトウェアの非公開部分についてのみ行なわれ、公開部分は暗号化検出回路によって検出され、そのままメモリにロードされる。このことにより、公開部分については、ユーザによって自由に改変・新規作成し、それをユーザ間で流用させることができる。このことは、たとえばゲーム用ソフトウェアにおいて、ゲームの基本的な動作を規定する雛型ソフトについては正規のユーザ以外の使用を防止し、ゲームの基本的動作に付加される各種の動作・効果を規定するカスタマズソフトについてはユーザが自由に開発し、それをユーザ間で流用させるソフトウェアの使用を実現する。

6

【００２８】上記請求項１に係る「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」は、いわば不正に複製されたソフトウェアの使用を起動の段階で防止するものであるのに対して、本願の請求項２に係る「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」は、正常に起動されたソフトウェアに対してメモリに直接アクセスしてプログラム・データを不正に参照するのを防止するようにしたものである。

【００２９】このために、請求項２に係る「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」では、初めにメモリ制御装置がソフトウェアの非公開部分をメモリ上の参照不可領域にロードし、公開部分をメモリ上の参照可能領域にロードし、アクセス制御手段によって、参照可能領域のプログラムあるいは外部のプログラムの実行による参照不可領域へのアクセスを禁止する。これにより、復号された状態でメモリ上に存在する非公開のプログラム・データへのアクセスが防止され、ソフトウェアの不正使用が防止される。

【００３０】本願請求項３に係る「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」は、上記請求項１または請求項２に係るシステムと同一の作用を有する他、ソフトウェア供給部とソフトウェア実行部が通信回線によって互いに連結されているので、ソフトウェア供給者は通信回線を通じて容易にユーザにソフトウェアを配布でき、また、ユーザは公開部分について変更あるいは新たに創作したものを通信回線を通じて容易にやり取りでき、かつ、非公開の雛型部分を正規に取得したユーザのみがそのやり取りされた公開部分を実行することができる。

【００３１】

【実施例】以下本発明の一実施例について添付の図面を用いて説明する。

【００３２】図１は本発明による「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」の一構成例を示している。本実施例のシステムは、通常一つのソフト供給部１と複数のソフトウェア実行部２ａ、２ｂ、２ｃ…とからなり、たとえば登録したユーザ（会員）にゲーム用ソフトウェアを断続して提供するようなものがこれに該当するので、理解容易のために以下このようなシステムを用いて説明する。この場合、ソフトウェア供給部１はソフトウェアを作成して会員に提供する業者側の装置に該当し、ソフトウェア実行部２ａ、２ｂ、２ｃ…はユーザ側の装置に該当する。

【００３３】本システムではゲーム用ソフトウェアの供給を受けるようとする者は、ソフトウェアを提供する業者に所定の手続によって申し出て会員として登録を受け

る。登録を受けると、その会員に固有の会員番号や暗証番号を含む認証情報がソフトウェア供給部1の認証情報テーブル3に登録され、ソフトウェアを実行するソフトウェア実行装置4と上記認証情報を格納した認証情報格納装置5を含む装置が会員に引き渡される。このソフト実行装置4と認証情報格納装置5は会員が所有するソフトウェア実行部2a、2b、2c…を構成する。

【0034】本実施例ではソフトウェア供給部1とソフトウェア実行部2a、2b、2c…は通線ネットワークによって結ばれており、互いにプログラムやデータをやりとりすることができるように構成されているが、フロッピーやROMやCD等の記憶媒体を介してプログラム・データをやりとりするように構成されていても良い。

【0035】このシステムにおいて、ソフトウェアの供給者は新作のソフトウェアを含む供給可能なソフトウェアを会員に知らせ、会員は使用したいソウフトウェアがあれば、ソウトウェア供給者に申し込んで供給を受ける。今、ソフトウェア実行部2bの会員が、所定のソフトウェアをソフトウェア供給者に申し込んだとすると、ソフトウェア供給部1では申込者の認証情報を認証情報テーブル3から取り出し、暗号化キー生成手段6によって所定の暗号化アルゴリズムに基づいて上記認証情報の暗号化キーを生成する。なお、上記暗号化アルゴリズムは後述するソフトウェア実行部2における復号化アルゴリズムと対応するものであるが、ユーザに対しては秘密にされる。

【0036】次にソフトウェア供給部1では、暗号化キー生成手段6によって生成された暗号化キーと申込みのあったソフトウェア7が暗号化手段8に入力され、暗号化される。ここで上記ソフトウェア7は、ゲームの基本的動作を規定し、改竄やコピーを許さない非公開の雛型ソフトと、雛型ソフト上で動くゲームの効果音や追加の動作のような、自由に創作してユーザ間で流用させる公開のカスタマイズソフトとからなる。ソフトウェア供給部1の暗号化手段8は、上記ソフトウェア7の雛型ソフトのみを暗号化し、カスタマイズソフトについては暗号化しない。したがって図1に示すようにソフトウェア7は、公開部分と暗号化部分を有する供給用ソフトウェア8bとして申込者に供給される。なお、暗号化キーが申込者によって異なるため、元が同一のソフトウェアであっても、その供給用ソフトウェア8a、8b、8c、はそれぞれ異なった内容を有する。

【0037】次に上記暗号化されたソフトウェアを復号化して実行するソフトウェア実行部2について詳細に説明する。

【0038】図2はソフトウェア実行部2の構成を示している。ソフトウェア実行部2は大きく分けてソフトウェアを実行するソフトウェア実行装置4と各ユーザの認証情報を格納したに認証情報格納装置5とからなる。ソフトウェア実行装置4は、さらに演算処理部9と、プログラムやデータをロードし演算処理部9の使用に供するメモリ10と、メモリ10に対するアドレス指定や参照等のアクセスを制御するメモリ制御装置11と、キーボード、マウス、ポインティングディバイス、ジョイスティック、タッチパネルなどの入力装置12と、表示装置13とからなる。

【0039】上記メモリ制御装置11は、ソフトウェアの暗号化部分と公開部分を検出する暗号化検出回路14と、認証情報格納装置5からの認証情報から復号化キーを生成して暗号化検出回路14によって検出された暗号化ソフトウェアを復号化するデータ復号化回路15と、メモリ10に対するアクセス命令の発信源を検出し、その発信源によってメモリ10へのアクセスを許可あるいは禁止するアクセス制御部16とを有している。

【0040】上記構成に基づいてソフトウェア実行部2の作用について以下に説明する。

【0041】供給用ソフトウェア8は、通信回線を介してソフトウェア実行部2の図示しない記憶装置に一旦格納され、あるいは記憶媒体に格納された状態でソフトウェア実行装置4の読込手段（図示せず）によってメモリ10に読み込まれる（この操作をロードという）。ソフトウェア実行装置4は、供給用ソフトウェア8が必ず暗号化検出回路14とデータ復号化回路15を経てメモリ10にロードされるようにハードウェア的に構成されている。暗号化検出回路14は、供給用ソフトウェア8の内容を検査し、公開部分すなわち非暗号化部分についてはそのままメモリ10の参照可能領域10aにロードする一方、供給用ソフトウェア8の暗号化された部分をデータ復号化回路15へ送る。

【0042】暗号化検出回路14による暗号化部分の検出はソフト的に暗号化された部分であることを示す信号を検出するようにしても良く、あるいはハード的に記憶媒体中の所定領域に格納されたプログラム・データを暗号化部分として検出するようにしても良い。

【0043】供給用ソフトウェア8の暗号化部分を入力したデータ復号化回路15は、認証情報格納装置5から認証情報を読み込み、この認証情報から所定の復号化アルゴリズムに基づいて復号化キーを生成し、この復号化キーによって暗号化されたプログラムやデータを復号化して、メモリ10の参照不可領域10bへロードする。

【0044】ここで上記復号化アルゴリズムは前記ソフトウェア供給部1の暗号化アルゴリズムと対応しており、同じく秘密にされている。

【0045】また、上記暗号化されたプログラムやデータの復号化は強制的に行われるものであり、認証情報の一致、不一致に拘らえず行われ、すでに解読された平文のプログラムやデータに対しても行なわれる。

【0046】これにより、仮に供給用ソフトウェア8が何らかの方法によって解読されて所定のユーザのソフトウェア実行部2で実行されようとする場合、データ復号

化回路１５によって解読されたプログラムやデータが強制的に再復号化され、意味をなさないものとなる。

【００４７】つまり、供給用ソフトウェア８を解読して所定のユーザのソフトウェア実行部２で実行可能にするには、ソフトウェアを解読し、かつ、そのユーザの復号化キーによって意味あるものに復号化されるように予め暗号化しておかなければならない。このような作業は使用されるユーザに一対一に行われなければならないので、大量の複製物の流出を防止することができる。

【００４８】さらに、ソフトウェアの暗号化アルゴリズムと復号化アルゴリズムはそれぞれ秘密にされており、特に暗号化アルゴリズムはソフトウェア供給部１に格納さているので、第三者がこれを知ることは極めて困難となる。

【００４９】上述したことはソフトウェアの起動時に不正に複製されたプログラムやデータについては正常に起動しないようにすることによってソフトウェアの不正使用を防止するようにしたものであるが、この他に本実施例のシステムによれば、正常に起動されたプログラムやデータに対してメモリに直接アクセスしてその内容を参照することを防止することができる。以下この機能について説明する。

【００５０】図２に示すように本実施例のソフトウェア実行装置４では、演算処理装置９がメモリ１０の参照可能領域１０ａあるいは参照不可領域１０ｂにロードされたプログラムを実行するが、メモリ１０に対するアクセス命令は必ずアクセス制御部１６を介するように構成されている。この場合、アクセス制御部１６はメモリ１０に対するアクセス命令が参照可能領域１０ａ参照不可領域１０ｂのいずれにロードされたプログラムの実行によって発せられているかを検知し、それによってメモリ１０に対するアクセスを許可あるいは禁止する。

【００５１】図３はアクセス制御部１６によってメモリ１０へのアクセスが許可・禁止される様子を模式的に示したものである。図３（ａ）はメモリ１０へのアクセス命令が参照不可領域１０ｂにロードされたプログラムの実行によって発せられた場合を示しており、この場合アクセス制御部１６はそのアクセス命令の発信源が参照不可領域１０ｂのプログラムであることを検知し、演算処理装置９による参照可能領域１０ａと参照不可領域１０ｂの双方へのアクセスを許可する。

【００５２】これに対して図３（ｂ）はメモリ１０へのアクセス命令が参照可能領域１０ａにロードされたプログラムの実行によって発せられた場合を示しており、この場合アクセス制御部１６は参照不可領域１０ｂへのアクセスを禁止し、参照可能領域１０ａへのアクセスを許可する。

【００５３】また、図３には示していないが、たとえばオペレーションシステム等の外部のプログラムによって直接演算処理装置９に対してメモリ１０へのアクセスを命令した場合、このアクセス命令は同様にアクセス制御部１６によって検知され、参照不可領域１０ｂ以外のプログラム命令としてメモリ１０へのアクセスが禁止される。

【００５４】上記アクセス制御部１６の作用により、ユーザは参照可能領域１０ａにおいて自由にカスタマイズソフトを作成できる一方、参照不可領域１０ｂにロードされる雛型ソフトを不正に複製・改竄することができなくなる。また、参照可能領域１０ａで作成されたカスタマイズソフトは暗号化されないで通信回線や記憶媒体を介して他のユーザのソフトウェア実行装置４で使用することができるようになる。

【００５５】

【発明の効果】上記説明から明らかなように本発明による「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」は、ソフトウェア供給部で各ユーザに固有の認証情報に基づいてソフトウェアの非公開部分を暗号化し、このソフトウェアをユーザのソフト実行部で暗号化検出回路によって暗号化部分を検出し、これをデータ復号化回路がそのユーザ固有の認証情報に基づいて復号化する。したがって正規のユーザに対しては非公開部分を有するソフトウェアを支障なく使用させることができる。またソフトウェアの公開部分については、暗号化せずにこれを暗号化検出回路によって検出し、そのままの状態で使用させるので改変あるいは新規に作成した公開のプログラムやデータをユーザ間で流用することができる。

【００５６】一方、一致しない認証情報やすでに解読されているプログラムやデータに対しては、上記データ復号化回路が強制的に復号化させるので意味をなさないものとすることができる。したがって特定のユーザにソフトウェアの非公開部分を支障なく使用させるには、その非公開のプログラムやデータを解読するのみならず、ソフトウェア供給者によって秘密にされている暗号化アルゴリズムに従って各ユーザの認証情報を用いて暗号化しなければならない。これは各ユーザに一対一の作業となるため、ソフトウェアの大量の複製・不正使用を防止することができる。

【００５７】また、本発明のシステムでは、アクセス制御部がメモリに対するすべてのアクセス命令を監視し、参照不可領域にロードされたプログラム、すなわちソフトウェア供給者が提供したプログラムの実行によるアクセス命令以外のメモリへのアクセスを禁止する。これにより、正常に作動しているプログラムやデータを参照することができなくなり、作動中のプログラムやデータの不正な複製等を防止することができる。

【００５８】上記構成要素とそれらの作用により、ソフトウェア供給者が内容を秘密にしようとするプログラムやデータについては正規のユーザにのみ使用させ、ユーザが創作した付加的なプログラムやデータはユーザ間で

自由に流用させることができる複数ユーザによる公開部分と非公開部分を有するソフトウェアの使用システムを得ることができる。

【図面の簡単な説明】

【図1】本発明による「公開部分と非公開部分を有するソフトウェアを複数ユーザに使用させるシステム」の全体構成を示した図。

【図2】ソフトウェア実行部の構成を示した図。

【図3】本発明のアクセス制御部の作用を模式的に示した図。

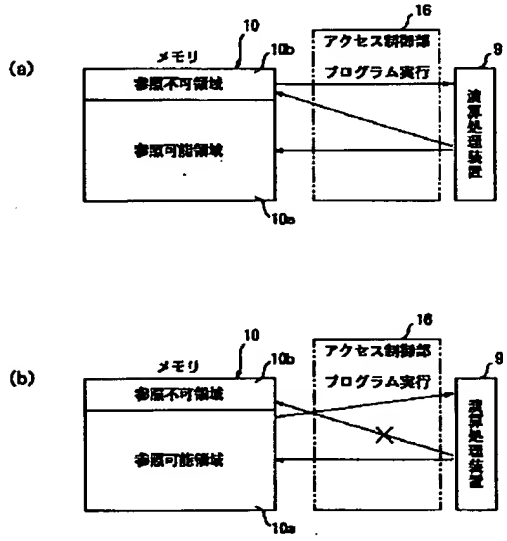
【図4】プログラムの一部に認証情報を付加する従来のソフトウェアを複数ユーザに使用させるシステムの構成を示した図。

【図5】ユーザが認証情報を入力して復号化する従来のソフトウェアを複数ユーザに使用させるシステムの構成を示した図。

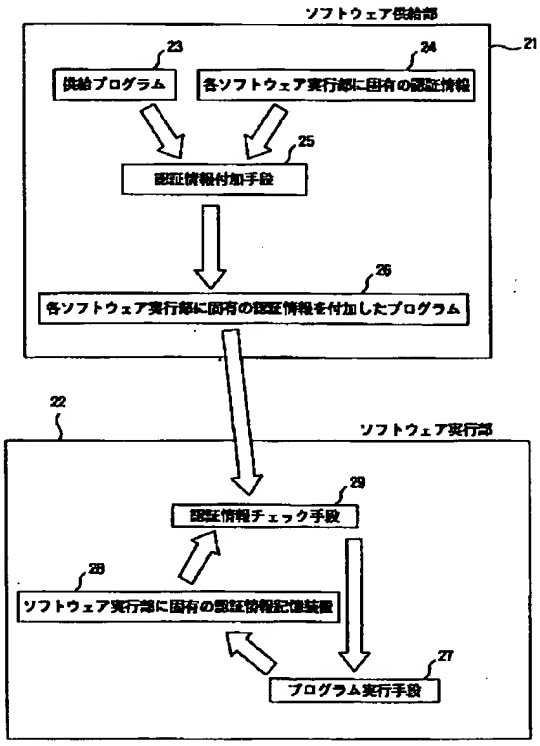
【符号の説明】

1　ソフトウェア供給部
2　ソフトウェア実行部
4　ソフトウェア実行装置
5　認証情報格納装置
6　暗号化キー生成手段
7　暗号化手段
9　演算処理装置
10　メモリ
11　メモリ制御装置
12　入力装置
13　表示装置
14　暗号化検出回路
15　データ復号化回路
16　アクセス制御部

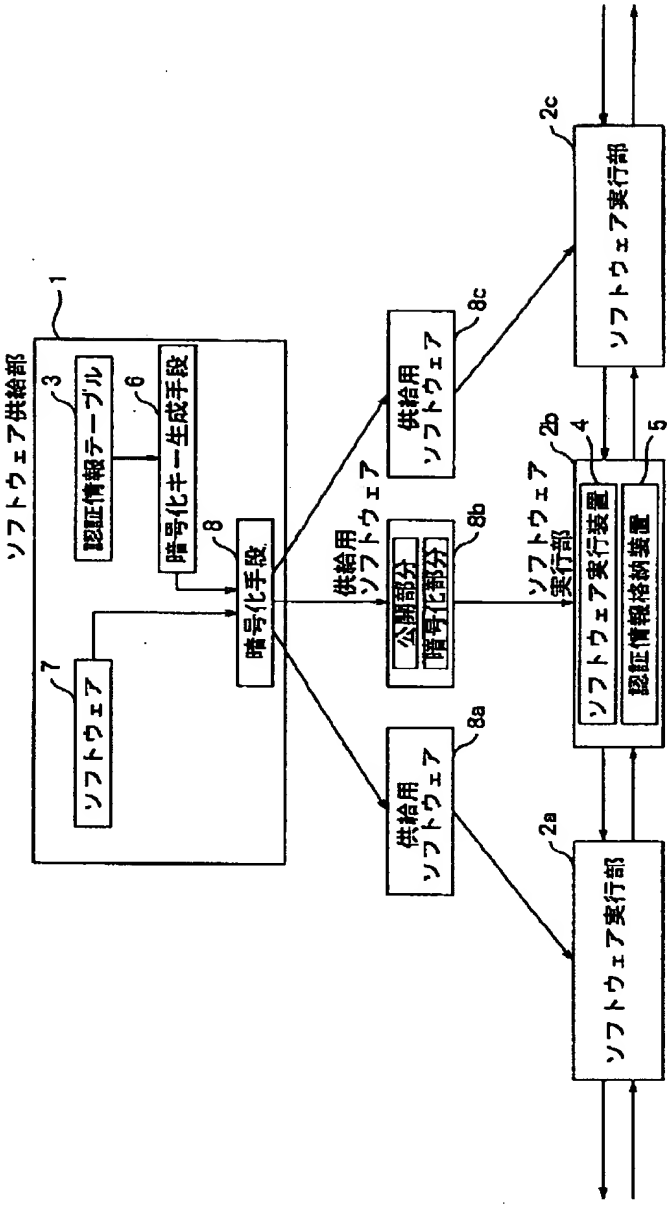
【図3】



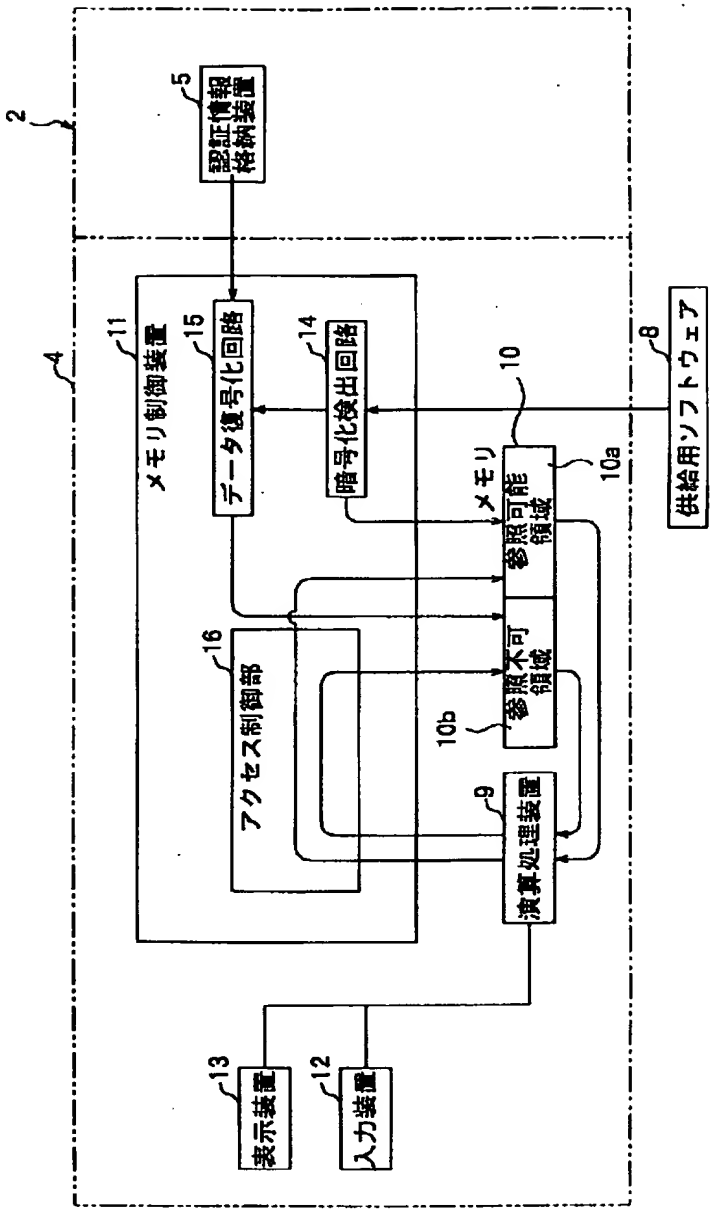
【図4】



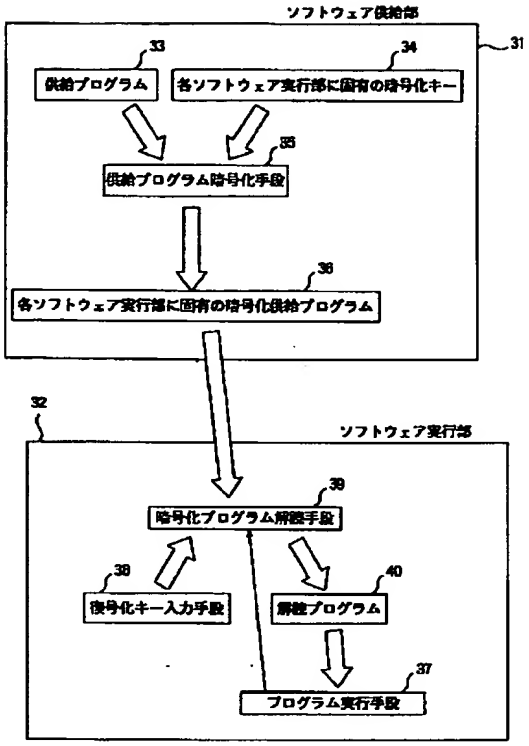
【図1】


ソフトウェア供給部
1
認証情報テーブル
3
暗号化キー生成手段
6
暗号化手段
8
ソフトウェア
7
供給用ソフトウェア
8c
供給用ソフトウェア
8b
公開部分
暗号化部分
供給用ソフトウェア
8a
ソフトウェア実行部
2b
ソフトウェア実行装置
4
認証情報格納装置
5
ソフトウェア実行部
2c
ソフトウェア実行部
2a

【図2】


2
5
認証情報格納装置
4
11
メモリ制御装置
15
データ復号化回路
14
暗号化検出回路
10
8
供給用ソフトウェア
メモリ
10a
参照可能領域
参照不可領域
10b
16
アクセス制御部
9
演算処理装置
13
表示装置
12
入力装置

【図5】


ソフトウェア供給部
31
33
供給プログラム
34
各ソフトウェア実行部に固有の暗号化キー
35
供給プログラム暗号化手段
36
各ソフトウェア実行部に固有の暗号化供給プログラム
32
ソフトウェア実行部
39
暗号化プログラム解読手段
38
復号化キー入力手段
40
解読プログラム
37
プログラム実行手段